

CLAIM SET AS AMENDED

1-12. (Canceled)

13. (Currently Amended) A method for copy protection, ~~decrypting an encrypted digital data file~~, comprising:

generating a data unit, the data unit including two portions, each of the two portions having a different protection level with respect to the other; and

transferring the data unit to a target device which has previously shared information for allowing transmission of the data unit.

~~receiving a reencrypted data file, wherein a portion of the reencrypted data file has been partially decrypted and reencrypted in a first decryption unit; and~~
~~using a second decryption unit to decrypt the received reencrypted data file, wherein the second decryption unit is different from the first decryption unit.~~

14. (Currently Amended) The method of claim 13, ~~wherein the partial decryption of~~
further comprising the step of partially decrypting the data unit ~~file is performed~~ at a plurality of locations spaced apart at a predetermined interval on the ~~data file~~ unit.

15. (Currently Amended) The method of ~~claim 13~~ claim 14, further comprising the step of storing the partially decrypted data file ~~unit~~ in a data storage medium or a digital data player.

16. (Currently Amended) The method of ~~claim 13~~ claim 14, further comprising the step of decrypting the a remainder of the partially decrypted data-file unit in the target device.

17. (Currently Amended) The method of -claim 13, wherein the data ~~file-unit~~ is partially decrypted based on a predetermined encryption key.

18. (Currently Amended) The method of claim 15, further comprising the step of reading the partially decrypted stored data ~~file-unit~~ from the data storage medium or the digital data player and reproducing the data-file unit at the request of a user.

19. (Currently Amended) The method of claim 18, further comprising the step of decrypting the data ~~file-unit~~ based on a predetermined encryption key, and outputting the decrypted data-file unit to an output line.

20. (Previously Presented) The method of claim 14, wherein the predetermined interval is a multiple or divisor of a buffer size.

21. (Currently Amended) A ~~digital data decryption system~~ for copy protection, comprising:

a computer adapted to generate a data unit, the data unit including two portions, each of the two portions having a different protection level with respect to the other; and

a target device for receiving the data unit after the target device has previously shared information for allowing transmission of the data unit.

~~a first receiving unit for receiving an encrypted digital data file;~~

~~a first decryption unit for decrypting a portion of the encrypted data file while leaving the remaining portion of the data file encrypted, thereby creating a partially decrypted data file; and~~

~~a second decryption unit for subsequently decrypting the partially decrypted data file.~~

22. (Currently Amended) The system of claim 21, ~~wherein the partial decryption of the data file received by the first receiving unit is performed~~ further comprising a first decryption unit in the computer for locating the two portions of the data unit at a plurality of locations spaced apart at a predetermined interval on the digital data file unit.

23. (Previously Presented) The system of claim 22, wherein the predetermined interval is a multiple or divisor of a buffer size.

24. (Currently Amended) The system of claim 21, further comprising a data storage medium associated with the ~~first receiving unit computer~~ for storing the partially decrypted data file unit.

25. (Currently Amended) The system of claim 21, wherein the data file unit received by the ~~first receiving unit computer~~ target device is partially decrypted based on a predetermined encryption key.

26. (Currently Amended) The system of claim 21, wherein the target device is a digital data playing device, further comprising a the digital data player playing device for receiving the ~~partially decrypted data file unit~~ from the computer, wherein the digital data ~~player playing~~ device includes ~~the a~~ second decryption unit.

27. (Currently Amended) A method for ~~decrypting an encrypted digital data file copy~~ protection, comprising:

registering a computer with a digital data server;
transferring an encrypted data unit from the server to the computer;
generating a partially decrypted data unit in the computer, the partially decrypted data unit including two portions which are encrypted at different levels with respect to each other;
receiving the encrypted data file in a first receiving unit;
transferring the encrypted data file to a first decryption unit;
using the first decryption unit to decrypt a portion of the data file received in the first receiving unit while leaving the remaining portion of the data file encrypted;
storing the decrypted data file in a buffer;
reencrypting the decrypted data file;

transferring the partially decrypted data unit to a target device having a second decryption unit; and
using a the second decryption unit for decrypting the ~~reencrypted~~ partially decrypted digital data-file unit.

28. (Currently Amended) The method of claim 27, wherein the step of partially decrypting ~~the portion of the encrypted data unit file received in the first receiving unit computer~~ is performed at a plurality of locations spaced apart at a predetermined interval on the ~~digital~~ partially decrypted data-file unit.

29. (Currently Amended) The method of claim 27, further comprising the step of storing the ~~reencrypted~~ partially decrypted data-file unit in a data storage medium ~~of or~~ a digital data player.

30. (Canceled)

31. (Currently Amended) The method of claim 27, wherein the ~~data-file unit~~ received by the ~~first receiving unit~~ target device is partially decrypted based on a predetermined encryption key.

32. (Currently Amended) The method of claim 29, further comprising the step of reading the partially decrypted stored data-file-unit from the data storage medium and reproducing the partially decrypted data unit ~~file-at-the-upon~~ request of a user.

33. (Currently Amended) The method of claim 32, further comprising the steps of: sending the ~~reencrypted~~ partially decrypted digital data file-unit to the digital data player; decrypting the reencrypted data ~~file-unit~~ based on a predetermined encryption key; and outputting the decrypted data ~~file-unit~~ to an output line of the digital data player.

34. (Canceled)

35. (Canceled)

36. (Currently Amended) The method of claim 27, further comprising the steps of: partially decrypting the encrypted data unit in the computer is performed independently of operating providing the first decryption unit in a computer; and ~~providing the second decryption unit in a separate the target device which operates independently from the computer;~~ wherein the partially decrypted data file is transferred from the computer to the separate device.

37. (Canceled)

38. (New) The method of claim 13, further comprising the steps of:

registering a computer with a data server;

transferring encrypted data from the data server to the computer to generate;

the data unit in a first decryption unit of the computer; and

using a second decryption unit of the target device and the shared information to decrypt

the data unit.

39. (New) The system of claim 21, further comprising:

a data server for transferring encrypted data from the data server to the computer, the

computer including a first decryption unit to generate the data unit based on the encrypted data,

wherein the target device receives the data unit from the computer, the target device

having a second decryption unit for decrypting the data unit using the shared information.